Section 2.4

Instruments and Control Systems

Contents

TABLES

Section 2.4
Instruments and Control Systems

2.4.1. Independent Protection Systems ITS

These are well bounded systems whose sole purpose is to prevent the process entering an undesirable state or returning the process to a desirable state from a potentially undesirable state. They are termed independent as they are independent from normal control and instrumentation systems. They are typically associated with radiological safety functionality but can be any of the following:

- Safety protection – automatic systems forming part of the hazard control strategy (see K70C514). Sometimes referred to as protective measures which consist of Safety Instrumented Systems sometimes supplemented by operator action known as operational preventative measures.

- Environmental protection – not part of safety protection but they automatically prevent damage to the environment from a hazard.

- Conventional safety protection – automatic systems preventing exposure of workers, co-located workers or public to conventional hazard.

- Loss prevention – not part of the hazard control strategy or environment protection but they automatically prevent costly damage to equipment or the quality of the product – typically not ITS.

Safety Instrumented Systems (SIS) consist of three parts: detection, decision and termination. The detection will consist of the primary measurement element plus associated electronics. The decision will consist of logic circuitry (e.g. relays) or software designed to meet predetermined logic. The decision logic will drive the termination device such as a trip solenoid valve. In order to increase the overall effectiveness of a protective measure the safety instrumented system may be supplemented with an operational preventative measure. This relies on operational plant control which allows corrective action to be taken in order to prevent an initiating event developing into an accident.

Those protective measures which perform safety protection by the use of CE&I SSCs are important to safety. They will form the part of Defense in Depth defined as ***Automatic Systems**:*

> "Automatic systems should be provided that would place and maintain the facility in a safe state and limit the potential spread of radioactive materials when operating conditions exceed predetermined safety set points." (DOE/RL-96-0006, Section 4.1.1.5).

These SSCs will have the following safety function:

- On detection of a state identifying a potential hazard, electrically isolate an action which causes or would contribute to the likelihood of the hazard.

The 0004 process will identify the importance of these SSCs to the control strategy which will lead to a configuration as defined by the appropriate standards:

Typical SIS configuration requirements for ITS Control and Instrumentation Systems will be comprised of one of the following:

1. A single means of:

   - detecting the onset of a hazard
   - deciding to take protective action and generating the necessary signals
   - terminating the event or reducing its consequence

2. At least two independent but not necessarily diverse means of:

   - detecting the onset of a hazard
   - deciding to take protective action and generating the necessary signals
   - terminating the event or reducing its consequence

No single failure should result in total loss of protection

3. At least two independent and diverse means of:

   - detecting the onset of a hazard
   - detecting to take protective action and generating the necessary signals
   - terminating the event or reducing its consequence

No single failure should result in total loss of protection.

2.4.2. Defense-in-Depth (Normal Instrumentation and Control)

These are the process instrumentation and control components that are configured to operate a process within its normal operating envelope. The major aspects of these systems are described below.

2.4.2.1. Instrumentation

This is the standard plant instrumentation for process measurement such as flow measurement and level measurement for process plant and position sensing for mechanical handling plant. It includes the measuring device, transducers, transmitters and other associated electronics. These SSCs will normally interface to a system for control or directly to an operator interface device for a non-automated plant.

2.4.2.2. Plant and Process Actuators

These are the standard SSCs that actuate to achieve the process requirements such as heating and pumping for process plant and motor drives for mechanical handling plant. It includes the actuating device and its control electronics. These SSCs will normally interface to a system for control or directly to an operator for a non-automated plant.

2.4.2.3. Integrated Control System (ICS)

The Integrated Control System (ICS) provides monitoring and control of the majority of the chemical process equipment and the mechanical handling systems. The ICS includes workstations within the central control room for remotely operated process plant. Where local residence of the operator is required for the process (e.g. import of feed materials) certain ICS operations will be achieved locally and workstations will be provided. Where line of site is required to aid operation, usually for mechanical handling plant, ICS operations will be local and workstations will be provided. Controllers will be situated around the plant buildings to interface to instrumentation, plant and process actuators and other, independent control systems. The ICS provides normal control of process parameters and will warn of reduced margins of safety and, where appropriate, automatically return the process into the designated safety operating regime. The controls included with the ICS will be selected and configured to control so as to keep parameters within their normal range.

2.4.2.4. Independent Control Systems

Certain control systems will be supplied independent of the ICS and will normally include a local workstation. These systems may be operated entirely locally or via the ICS depending on the operating requirements of the system. In either case, the ICS will monitor their operation to identify trouble with the system.

2.4.2.5. Normal Control as a Component of Defense in Depth

The normal control and instrumentation will form the part of Defense in Depth defined as ***Control***: "Normal operation, including anticipated operational occurrences, maintenance and testing, should be controlled so that facility and system variables remain within their operating ranges and the frequency of demands placed on structures, systems and components important to safety is small" (K70C514).

The control and instrumentation SSCs will be designed to meet this criterion in order to control the process for operability rather than safety reasons. It will therefore be designed to keep the process parameters and operations within the design envelope.

2.4.3. Independent Detection and Alarm Systems

These are detection and alarm systems in addition to normal control and instrumentation which may be required for the same reasons as those defined for Independent Protection Systems in Section 2.4.1. Those independent detection and alarm systems which perform safety protection by the use of CE&I SSCs are important to safety.

- To alarm to local personnel of the onset of a hazard so that they may leave the area or take some other mitigating action. Alpha-in-Air, Beta-in-Air and Gamma Radiation monitoring meet typical requirements for these systems.

- These systems support attenuation of the consequences of an accident defined as the mitigation aspects of defense in depth. The safety functions of these alarm systems is to alarm when detecting the dangerous consequences of an accident so that personnel may take action to reduce the consequences to themselves, co-located workers or the public.

2.4.4. Plant Wide Systems (non-alarm)

These are systems used for overall plant administrative purposes. They include:

- Building Access Control for control of access via automatic barriers and central monitoring of building access. Its purpose is for overall building security.
- Public address system for broadcast communication to plant areas.
- Telephone system for person to person communications.

These systems have no specific safety function but are required for the overall operation of the facility. They have no specific design safety features.

2.4.5. Instrument and Control Design

2.4.5.1. Important to Safety SSCs

For the ITS independent protection systems and independent alarm systems described above the following Design Safety Features are generic and are not mentioned specifically in the tables.

Identification	A means of clearly identifying to plant personnel that the design purpose of the SSC is important to safety. This may be achieved by labeling, color coding or comments within software.
Independence	An SSC made up of detection, decision and trip termination components separate from normal instrumentation and control.
Periodic functional test	Tests performed on an important to safety SSC at a set interval throughout operational life of plant to detect failures in the SSC so that it may be restored to an “as new” condition or as close as practical.
Proven technology	Use of SSCs and techniques equivalent to those applied regularly and successfully in industrial applications (e.g. nuclear, process, manufacturing industries)

The following Design Safety Features are commonly used depending on their appropriateness to the design, the availability of the function for the given technology and on the required reliability or availability.

Battery backed	A supplemental power supply to an electrically operated SSC which automatically switches to supplemental power supply without interruption of power to the SSC in the event of a loss of the primary electrical power supply. This may be achieved via an integral battery system or by utilizing one of the plant Uninterruptible Power Supplies.
Diversity	Use of different technologies, equipment or design methods to perform a common function with the intent to minimize common model cause faults. Applicable common cause events are identified in Section 2.10.2.
Fail safe	The capability to go to a predetermined safe state in the event of a specific malfunction.
Inspection	In addition to the formal proof testing, a process variable being measured as an input to an important to safety SSC may be regularly inspected in order to give confidence in the continued correct operation of the sensing instrument.
Redundancy	In an item, the existence of more than one means for performing a required function. Provision of duplicate ITS SSCs to ensure the performance of an ITS function. Need for redundancy determined by hazard analysis during design to prevent common mode/common cause faults.
Self-checking	An SSC with the built-in capabilities to periodically verify its own function, such that its normal function is confirmed without the need to interrupt operation for manually assisted checks (such as Periodic Functional Tests)
Separation	Installation of redundant and/or diverse ITS SSCs and support systems in location and along routes which would allow the maintenance of one system in the event of loss of the other due to some DBA. Separation is used to guard against common mode failure of a system.
Trouble alarm	Visual and/or audible notification to plant personnel that an ITS SSC has detected some form of failure which may be degrading its operation and maintenance is required.

2.4.5.2. Defense in Depth SSCs

The following Design Features would normally be applied on the Instrument and Control Design as good engineering practice. No formal credit is taken for these features as control strategies in attempting to reach the target reliability but they are an aspect of the engineering approach to Defense in Depth.

Control System Trips and Interlocks	The tripping or interlocking function may be achieved within the normal control and instrumentation with the intention of operating so that no demand would normally be placed on a Safety Instrumented System.
Trip Verification Sequences	The normal control system may verify the correct operation of the trip by monitoring its inputs and outputs and alarming on identification of a discrepancy between control system logic and Safety Instrumented System logic.

2.4.6. Hazardous Situations

Individual hazardous situations requiring the use of ITS control and instrumentation are identified in the individual generic system fault table.

The following table represents typical fault conditions contained in the generic system tables and the ITS Instrumentation and Control SSCs for those faults.

Table 2.4-1. I&C Important to Safety SSCs.

Fault	Important to Safety SSCs	Safety Function	Design Safety Features
Loss of confinement causing contamination of cooling water	Gamma monitor Decision Logic circuitry Isolation valve(s)	Detect abnormal activity levels in CW loop Stop pump Isolate CW loop	Trouble alarm Redundancy where required by analysis Inspection
Loss of confinement causing radiation release	Airborne radiation monitor (gamma) with integral alarm Power supply	Warn personnel of radiation hazard in vicinity	Trouble alarm Inspection Battery backed
Loss of confinement causing radiation release	Continuous area monitor (alpha & beta) with integral alarm Power supply	Warn personnel of radiation hazard in vicinity	Trouble alarm Inspection Battery backed
Loss of confinement causing excessive atmospheric effluent release	Monitor sample pump(s) CCR Alarms Power Supply	Central Control Room Alarm Record Discharge continuously	Self checking where analysis requires Diversity where required by analysis Trouble Alarm Battery Backed
Loss of confinement causing excessive liquid effluent release	Gamma monitor Logic circuit CCR alarms Isolation valves	Isolate discharge Central Control Room Alarm	Redundancy where required by analysis Self checking where required by analysis Trouble alarm
Attempt to open shield door with source present	Radiation Monitoring Decision Logic and circuitry Electrical isolating device Warning light	Prevent door opening when radiation exceeds limits Prevent door opening when radiation exceeds limits Warn of high radiation	Redundancy where required by analysis Diversity where required by analysis Separation where required by analysis Battery backed warning light

Fault	Important to Safety SSCs	Safety Function	Design Safety Features
Overfilling a vessel	Level Instrumentation Instrument air supply, if a pneumatic dip tube measurement is used Logic circuitry Final Control Device	Isolate Feed	Inspection Redundancy where required by analysis Separation if required by analysis Diversity when required by analysis If dip system is used, air purge prevents back flow; however, loss of air will initiate isolation of air supply
Loss of primary confinement (leak)	Detection Instruments Logic circuitry Isolation valves and actuators Air supply instruments, if a pneumatic dip tube measurement is used	Isolate feed sources	Inspection Redundancy where required by analysis Separation when required by analysis Diversity when required by analysis If dip system is used, air purge prevents back flow; however, loss of air will initiate isolation of air supply
Loss of confinement (hazardous vapors)	Detection instruments Local Alarm	Detect buildup above acceptable limits Local Alarm Actuation Mitigation action based on hazard. To be determined by analysis	Battery backed Intrinsically safe circuitry if required by analysis Trouble alarm

Fault	Important to Safety SSCs	Safety Function	Design Safety Features
Overheating	Temperature measurement Power supply Alarm	Mitigation action based on hazardous analysis	Inspection Trouble alarm Battery backed
Over Pressure	Pressure measurement Power supply Alarm	Mitigation action based on hazardous analysis	Inspection Trouble alarm Battery backed
Fan failure	Measurement Instrumentation Logic circuitry Electrical isolating device	Detect loss of extract Fan Shutdown inlet system	Inspection Redundancy where required by analysis Separation where required by analysis Diversity where required by analysis Trouble alarm
Fan failure (Loss of Depression in C5)	Measurement instrumentation Logic circuitry Electrical tripping device	Detect loss of cell depressurization Trip isolation dampers	Inspection Redundancy where required by analysis Separation where required by analysis Diversity where required by analysis Trouble alarm
Filter Failure	Detection Instrumentation Logic circuitry Electrical tripping device	Transfer to standby filter	Inspection Redundancy where required by analysis Separation if required by analysis Diversity if required by analysis Trouble alarm
Fire	Fire Detection Logic circuitry Electrical tripping device	Isolate air inlet to fire location	Trouble alarm

Fault	Important to Safety SSCs	Safety Function	Design Safety Features
Both shield doors open at same time	Position sensors Logic circuitry Electrical isolating device	Prevent opening of inner and outer shield doors between caves and operator areas	Redundancy where required by analysis Separation where required by analysis Diversity if required by analysis
Released/dropped load	Load Cells Logic circuitry Load release controls	No load release for out of cell delivery cranes.	Diversity if required by analysis
Failure to operate or spurious operation of shield door	Alpha and beta in air detectors	Detect high activity in air	Multiple elements Continuous test signal system Trouble/failure alarm system
	Alarms	Alert operators to evacuate	Multiple. Audible and visual Trained and rehearsed operator
	Power	Operate system	UPS, dedicated battery system
	Logic	Effect appropriate level of response to detected hazard level	Fault tolerant PLC under procedural change and testing control. Local monitors and alarms still operate on failure of system logic. Monitors under calibration are outside
	External warning lights	Alert operators not to enter	Application of Multiple Warning